

Hashcat

<https://github.com/hashcat/hashcat>

Written by Justin Wang || [linkedin.com/in/hsiaoan-wang-4514ab45/](https://www.linkedin.com/in/hsiaoan-wang-4514ab45/)
Revised by Kent Ickler || [X @krelkci](#)

Hashcat is a powerful tool for recovering lost passwords, and, thanks to GPU acceleration, it's one of the fastest. It works by rapidly trying different password guesses to determine the original password from its scrambled (hashed) version. Hashcat uses various clever techniques, like dictionary attacks (testing common passwords), leetspeak tricks (e.g., replacing "e" with "3"), pattern-based guessing, and combining different words or phrases. This helps expose weak passwords and poor security habits, which many people rely on when configuring and registering accounts online. Because of its effectiveness, Hashcat is widely used in cybersecurity training, ethical hacking, and penetration testing to improve password security and help organizations strengthen their defenses.

```
hashcat -m <mode> -a <attack> <file storing your hash> <path to wordlist/mask>
```

Commonly Used Modes (-m)

0	MD5	1000	NTLM
900	MD4	1100	Domain Cached Credentials (DCC), MS Cache
1700	SHA2-512	1800	sha512crypt \$6\$, SHA512 (Unix)
10	MD5 (\$pass.\$salt)	3000	LM
20	MD5 (\$salt.\$pass)	5700	Cisco-IOS type 4 (SHA256)
110	SHA1:salt	7400	sha256crypt \$5\$, SHA256 (Unix)
120	SHA1:pass	8100	Citrix NetScaler (SHA1)
2600	md5(md5(\$pass))	12800	MS-AzureSync PBKDF2-HMAC-SHA256
4500	sha1(sha1(\$pass))	131	MSSQL (2000)
400	phpass	132	MSSQL (2005)
8900	scrypt	200	MySQL323
2500	WPA/WPA2	300	MySQL4.1/MySQL5
2501	WPA/WPA2 PMK	1731	MSSQL (2012, 2014)
4800	iSCSI CHAP authentication, MD5(CHAP)	1600	Apache \$apr1\$ MD5, md5apr1, MD5 (APR)
5500	NetNTLMv1 / NetNTLMv1+ESS	8300	DNSSEC (NSEC3)
5600	NetNTLMv2	15000	FileZilla Server > 0.9.55
7500	Kerberos 5, etype 23, AS-REQ Pre-Auth	22100	Bitlocker
7300	IPMI 2 RAKP HMAC-SHA1	22400	AES Crypt (SHA256)
7350	IPMI2 RAKP HMAC-MD5	29521	LUKS v1 SHA-256 + AES
13100	Kerberos 5, etype 23, TGS-REP	9500	MS Office 2010
18200	Kerberos 5, etype 23, AS-REP	9600	MSOffice 2013
19600	Kerberos 5, etype 17, TGS-REP	5200	Password Safe v3
19700	Kerberos 5, etype 18, TGS-REP	6800	LastPass + LastPass sniffed
19800	Kerberos 5, etype 17, Pre-Auth	13400	KeePass 1 (AES/Twofish) and KeePass 2 (AES)
19900	Kerberos 5, etype 18, Pre-Auth	29700	KeePass 1 (AES/Twofish) and KeePass 2 (AES) - keyfile only mode
27000	NetNTLMv1 / NetNTLMv1+ESS (NT)	11600	7Zip
27100	NetNTLMv2 (NT)	13600	WinZip
27300	SNMPv3 HMAC-SHA512-384		
28900	Kerberos 5, etype 18, DB		

Attack Modes (-a)

0 = Straight Dictionary Attack

Example: `hashcat -m 500 -a 0 hash.txt dict.txt`

1 = Combination Attack

Example: `hashcat -m 500 -a 1 hash.txt dict1.txt dict2.txt`

3 = Brute Force Attack

Example: `hashcat -m 500 -a 3 hash.txt ?l?d?u`

6 = Hybrid Wordlist + Mask

Example: `hashcat -m 500 -a 6 hash.txt wordlist.txt ?d?s`

7 = Mask + Wordlist

Example: `hashcat -m 500 -a 7 hash.txt ?d?s wordlist.txt`

Useful Command Arguments

<code>--runtime=X</code>	Abort session after X seconds of runtime.
<code>--session=X</code>	Define session name to be string X.
<code>--restore</code>	Restore session from --session.
<code>-o</code>	Define output file for recovered hash.
<code>--show</code>	Show the cracked hashes.
<code>--left</code>	Show the uncracked hashes.
<code>--username</code>	Enable ignoring of usernames in hashfile.
<code>--remove</code>	Enable removal of hashes once they are cracked.
<code>-b</code>	Run benchmark of selected hash modes.

Mask Character Sets (?)

<code>?l</code>	abcdefghijklmnopqrstuvwxyz
<code>?u</code>	ABCDEFGHIJKLMNOPQRSTUVWXYZ
<code>?d</code>	123456789
<code>?h</code>	0123456789abcdef
<code>?H</code>	0123456789ABCDEF
<code>?s</code>	!"#\$%&'()*+,-./:;<=>?@[\]^_`{ }~
<code>?a</code>	?l?u?d?s
<code>?b</code>	0x00 - 0xff

Example: `hashcat -m500 -a 3 hash.txt ?l?l?a?a?a?a?d?d`

Brute force cracking using the masks to check for passwords that have 2 lowercase letters, 4 characters of all possibilities, and 2 numbers.



For a more expansive cheatsheet, check this out:

<https://www.blackhillsinfosec.com/wp-content/uploads/2020/09/HashcatCheatSheet.v2018.1b.pdf>